日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてい る事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年１０月 ６日

出 願 番 号
Application Number: 特願２０００－３０７８２２

出 願 人
Applicant (s): 村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ３月２３日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２００１－３０２３００２

【書類名】　特許願

【整理番号】　21573

【提出日】　平成12年10月 6日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04K 1/00

【発明の名称】　暗号化方法，復号方法，暗号通信方法，暗号通信システム及び記録媒体

【請求項の数】　10

【発明者】

【住所又は居所】　滋賀県大津市仰木の里東８丁目７－１２

【氏名】　片柳　磨子

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫
【電話番号】　06-6944-4141
【選任した復代理人】
【識別番号】　100114557
【弁理士】
【氏名又は名称】　河野　英仁
【電話番号】　06-6944-4141
【手数料の表示】
【予納台帳番号】　001889
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9805283
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法，復号方法，暗号通信方法，暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項１】　平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなるｋ個の成分を有する第１ベクトル、ｎ個の任意の乱数を成分とする第２ベクトル、及び、前記ｋ個の成分または前記ｎ個の成分の位置を特定する情報を示すｈ個の成分を有する第３ベクトルを加えたＫ（＝ｋ＋ｎ＋ｈ）個の成分を有する第４ベクトルと、公開されている第５ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項２】　前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第４ベクトルにおける前記ｈ個の成分の位置は同一である請求項１に記載の暗号化方法。

【請求項３】　前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記ｋ個の成分に応じて次のブロックでの前記第４ベクトルにおける前記ｋ個の成分または前記ｎ個の成分の位置を決定する請求項１に記載の暗号化方法。

【請求項４】　前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる１つのブロックと、前記第３ベクトルのｈ個の成分を平文を分割してなるｈ個の成分に置き換えた前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記ｋ個または（ｋ＋ｈ）個の成分に応じて次のブロックでの前記第４ベクトルにおける（ｋ＋ｈ）個の成分または前記ｎ個の成分の位置を決定する請求項１記載の暗号化方法。

【請求項５】　前記第５ベクトルは、１または複数組の整数d_i（$1 \leqq i \leqq K$）及び乱数v_iを用いて各組毎にＫ個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1 \ d_2 \cdots d_K$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された１または複数の第６ベクトルとを用いて生成する請求項１～４の何れ

かに記載の暗号化方法。

【請求項６】　前記第４ベクトルの各成分と、前記第６ベクトルを基にモジュラ変換した前記第５ベクトルの各成分とによる積和演算により暗号文を得るようにした請求項５に記載の暗号化方法。

【請求項７】　請求項１～６の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記第１ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする復号方法。

【請求項８】　第１のエンティティ側で、請求項１～６の何れかに記載の暗号化方法に従って平文から暗号文を作成して第２のエンティティ側へ伝送し、伝送された暗号文を該第２のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、平文を分割してなる前記ｋ個もしくは（ｋ＋ｈ）個の成分または前記ｎ個の成分の位置を前記一方のエンティティ側で任意に決定することを特徴とする暗号通信方法。

【請求項９】　両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～６の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第１のエンティティから第２のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項１０】　コンピュータに、平文から積和型の暗号文を得させるためのプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなるｋ個の成分を有する平文ベクトル、ｎ個の任意の乱数を成分とする疑似平文ベクトル、及び、前記ｋ個の成分または前記ｎ個の成分の位置を特定する情報を示すｈ個の成分を有する位置特定ベクトルを加えたＫ（＝ｋ＋ｎ＋ｈ）個の成分を有する伸長平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、得られた前記伸長平文ベクトルと公開された公開鍵ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系に関し、特に、積和型暗号に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を平文に復号す

る。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_K）と公開鍵である基数ベクトルｃ＝（c_1，c_2，・・・，c_K）とを用いて、暗号文Ｃ＝m_1 c_1 ＋m_2 c_2 ＋・・・＋m_K c_K を作成し、受信者である他方のエンティティ側でその暗号文Ｃを秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化方式である。

【０００７】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、中国人の剰余定理を用いることにより、高速な並列復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特開2000－89669 号）。この暗号化方法は、基数ベクトルｃの成分c_i （ｉ＝１，２，・・・，Ｋ）を、互いに素なＫ個の整数d_i を用いてD_i ＝ｄ／d_i （但し、ｄ＝d_1 d_2 ・・・d_K ）に設定した基数D_i を基にモジュラ変換したもの、または、互いに素なＫ個の整数d_i，乱数v_i を用いてD_i ＝（ｄ／d_i ）v_i に設定した基数D_i を基にモジュラ変換したものにすることを特徴としている。このようにして、中国人の剰余定理を用いて並列に復号するので、高速な復号を行うことができる。

【０００８】

【発明が解決しようとする課題】

しかしながら、この方式では、公開鍵の数を非常に大きくしない限り低密度であるので、ＬＬＬ（Lenstra-Lenstra-Lovasz）アルゴリズムを用いて公開鍵と暗号文とから直接平文を求める低密度攻撃に弱い場合があるという問題があり、安全性の面での更なる改良が望まれている。

【０００９】

本発明は斯かる事情に鑑みてなされたものであり、上記従来例を改良して低密度攻撃に強く、安全性を向上できる暗号化方法及び復号方法、この暗号化方法を用いる暗号通信方法及び暗号通信システム、並びに、この暗号化方法の動作プログラムを記録した記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】

請求項１に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を分割してなるｋ個の成分を有する第１ベクトル、ｎ個の任意の乱数を成分とする第２ベクトル、及び、前記ｋ個の成分または前記ｎ個の成分の位置を特定する情報を示すｈ個の成分を有する第３ベクトルを加えたＫ（＝ｋ＋ｎ＋ｈ）個の成分を有する第４ベクトルと、公開されている第５ベクトルとを用いて暗号文を得ることを特徴とする。

【００１１】

請求項２に係る暗号化方法は、請求項１において、前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、各ブロックにおいて、前記第４ベクトルにおける前記ｈ個の成分の位置は同一であることを特徴とする。

【００１２】

請求項３に係る暗号化方法は、請求項１において、前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックから構成されており、前のブロックでの前記ｋ個の成分に応じて次のブロックでの前記第４ベクトルにおける前記ｋ個の成分または前記ｎ個の成分の位置を決定することを特徴とする。

【００１３】

請求項４に係る暗号化方法は、請求項１において、前記暗号文は、前記第４ベクトルと前記第５ベクトルとを用いて得られる１つのブロックと、前記第３ベクトルのｈ個の成分を平文を分割してなるｈ個の成分に置き換えた前記第４ベクトルと前記第５ベクトルとを用いて得られる複数のブロックとから構成されており、前のブロックでの平文を分割してなる前記ｋ個または（ｋ＋ｈ）個の成分に応じて次のブロックでの前記第４ベクトルにおける（ｋ＋ｈ）個の成分または前記ｎ個の成分の位置を決定することを特徴とする。

【００１４】

請求項５に係る暗号化方法は、請求項１～４の何れかにおいて、前記第５ベクトルは、１または複数組の整数d_i（$1 \leqq i \leqq K$）及び乱数v_iを用いて各組毎にＫ個の各成分V_iが$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1\ d_2 \cdots d_K$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された１または複数の第６ベクトルとを用いて生成することを特徴とする。

【００１５】

請求項６に係る暗号化方法は、請求項５において、前記第４ベクトルの各成分と、前記第６ベクトルを基にモジュラ変換した前記第５ベクトルの各成分とによる積和演算により暗号文を得るようにしたことを特徴とする。

【００１６】

請求項７に係る復号方法は、請求項１～６の何れかに記載の暗号化方法を用いて得られた暗号文を復号する復号方法であって、前記第１ベクトルの成分の位置を同定しながら、前記暗号文を平文に復号することを特徴とする。

【００１７】

請求項８に係る暗号通信方法は、第１のエンティティ側で、請求項１～６の何れかに記載の暗号化方法に従って平文から暗号文を作成して第２のエンティティ側へ伝送し、伝送された暗号文を該第２のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法であって、平文を分割してなる前記ｋ個もしくは（ｋ＋ｈ）個の成分または前記ｎ個の成分の位置を前記一方のエンティティ側で任意に決定することを特徴とする。

【００１８】

請求項９に係る暗号通信システムは、両エンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～６の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を第１のエンティティから第２のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備えることを特徴とする。

【００１９】

請求項10に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムを記録してあるコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を分割してなるｋ個の成分を有する平文ベクトル、ｎ個の任意の乱数を成分とする疑似平文ベクトル、及び、前記ｋ個の成分または前記ｎ個の成分の位置を特定する情報を示すｈ個の成分を有する位置特定ベクトルを加えたＫ（＝ｋ＋ｎ＋ｈ）個の成分を有する伸長平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、得られた前記伸長平文ベクトルと公開された公開鍵ベクトルとを用いて暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むコンピュータプログラムを記録してあることを特徴とする。

【００２０】

本発明では、平文に冗長性を持たせる、言い換えると平文を退化させて暗号文を作成する。即ち、暗号化すべき平文を分割してなる第１ベクトル（平文ベクトル）、特に暗号化を必要としない乱数成分からなる第２ベクトル（疑似平文ベクトル）、及び、第１ベクトルまたは第２ベクトルの各成分の位置を示す第３ベクトル（位置特定ベクトル）を合わせた第４ベクトル（伸長平文ベクトル）と、公開されている第５ベクトル（公開鍵ベクトル）とを用いて暗号文を作成する。具体的には、第４ベクトル（伸長平文ベクトル）の各成分と、１または複数の第６ベクトル（基数ベクトル）を基にモジュラ変換した第５ベクトル（公開鍵ベクトル）の各成分との積和演算によって暗号文を構成する。この際、第１ベクトルまたは第２ベクトルの各成分の位置は、暗号文を作成する送信側のエンティティで決定する。また、第３ベクトルの各成分の位置は公開とする。

【００２１】

本発明では、暗号化が必要でない冗長部分（退化部分）を付加しているため、暗号文の密度が高くなり、また、１つの第１ベクトル（平文ベクトル）に対して非常に多数の第４ベクトル（平文ベクトル）つまり非常に多数の暗号文が存在するので、ＬＬＬアルゴリズムに基づく低密度攻撃は非常に困難となる。この結果、安全性が向上する。また、本来の暗号化すべき平文部分である第１ベクトル（平文ベクトル）の各成分の位置、または、冗長部分（退化部分）である第２ベクトル（疑似平文ベクトル）の各成分を付加する位置は、固定でなく、送信側のエンティティが任意に決定できる。この位置情報は第３ベクトル（位置特定ベクトル）として暗号文に盛り込まれて、受信側のエンティティへ伝送され、その第３ベクトルの各成分の位置は公開されているので、受信側のエンティティにて、第３ベクトルの成分が復号され、その復号結果に基づき第１ベクトル（平文ベクトル）の各成分の位置が分かって、平文に復号できる。本発明では、このように平文部分の位置または冗長部分（退化部分）の付加位置が固定でなく、送信側のエンティティにて決定するため、その位置が攻撃者には未知であるため、安全性は向上する。

【００２２】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

まず、本発明の説明に用いる幾つかの定義について説明する。本発明にあっては、暗号化すべき平文は幾つかの分割平文に分けられる。各分割平文をメッセージベクトルｍとして扱う。以下に定義する伸長変換によって、メッセージベクトルｍはベクトルｍ′に伸長される。このベクトルｍ′を、伸長メッセージベクトルと称する。これらのベクトルｍ，ベクトルｍ′の各成分のビットサイズの和を夫々ε（ビット），ε′（ビット）（但し、ε≦ε′）とする。また、暗号文が取り得る最大ビット数をC_{max}とする。

【００２３】

〈定義１（密度）〉

方式密度ρを下記（１）のように定義する。

【００２４】

【数１】

$$\rho = \frac{\varepsilon'}{\log_2 C_{max}} \quad \cdots \quad (1)$$

【００２５】

〈定義２（レート）〉

レートηを下記（２）のように定義する。

【００２６】

【数２】

$$\eta = \frac{\varepsilon}{|C_{max}|} \quad \cdots \quad (2)$$

【００２７】

ベクトル$a=(a_1, a_2, \cdots, a_w)$をｗ次元ベクトルとし、ベクトル$c=(c_1, c_2, \cdots, c_n)$をｎ次元ベクトルとする。また、ベクトル$b=(b_1, b_2, \cdots, b_n)$を重みｗのｎ次元２値ベクトルとする。但し、下記（３）の条件を満たす。

【００２８】

【数３】

$$\left.\begin{array}{l} b_{i_1} = b_{i_2} = \cdots = b_{i_w} = 1 \\ i_1 < i_2 < \cdots < i_w \end{array}\right\} \quad \cdots \quad (3)$$

【００２９】

〈定義３（添数集合）〉

添数集合Ｉ＝Ｉｎｄ（ベクトルｂ）を下記（４）のように定義する。

$$I = \{i_1, i_2, \cdots, i_w\} \quad \cdots (4)$$

【００３０】

〈定義４（ベクトル表現）〉

添数集合Ｉは、｛１，２，・・・，ｎ｝の部分集合であり、ベクトル表現として、ベクトルｄ＝Ｖｅｃ（Ｉ，ｎ）を下記（５）のように定義する。但し、ベクトルｄ＝（d_1，d_2，・・・，d_n）であり、例えば、Ｉ＝Ｉｎｄ（ベクトルｂ）である場合に、ベクトルｂ＝Ｖｅｃ（Ｉ，ｎ）である。

【００３１】

【数４】

$$d_i = \begin{cases} 1 & (i \in I) \\ 0 & (i \notin I) \end{cases} \quad \cdots \quad (5)$$

【００３２】

〈定義５（伸長）〉

ベクトルｂによりベクトルａから伸長されたｎ次元ベクトルｃは、ベクトルｃ＝ベクトルａ｛ベクトルｂ｝にて表記し、下記（６）のように定義する。例えば、ベクトルａ＝（a_1，a_2，a_3），ベクトルｂ＝（１，０，１，１）である場合に、ベクトルａ｛ベクトルｂ｝＝（a_1，０，a_2，a_3）となる。

【００３３】

【数５】

$$\begin{cases} c_{ij} = a_j \\ c_k = 0 \quad (b_k = 0 \text{ の場合}) \end{cases} \quad \cdots \quad (6)$$

$$(j = 1, 2, \cdots, w \ 、\ k = 1, 2, \cdots, n)$$

【００３４】

〈定義６（抜き出し）〉

ベクトルｂによりベクトルｃから抜き出されたｗ次元ベクトルａは、ベクトル

ａ＝ベクトルｃ｛ベクトルｂ｝にて表記し、下記（７）のように定義する。例えば、ベクトルｃ＝（c_1，c_2，c_3，c_4），ベクトルｂ＝（１，０，１，１）である場合に、第１，第３及び第４成分が抜き出されて、ベクトルｃ｛ベクトルｂ｝＝（c_1，c_3，c_4）となる。

【００３５】

【数６】

$$\vec{a} = (c_{i_1}, c_{i_2}, \cdots, c_{i_w}) \cdots (7)$$

【００３６】

次に、本発明の具体的な方式について説明する。

図１は、本発明による暗号化方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａが、暗号化器１にて平文ｘを暗号文Ｃに暗号化し、通信路３を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂが、復号器２にてその暗号文Ｃを元の平文ｘに復号する場合を示している。

【００３７】

〈平文分割〉

平文ｘは、ｅｋビットの複数のブロックに分割される。各ブロックは下記（８）のようにメッセージベクトルｍで表現される。なお、m_i（ｉ＝１，２，・・・，ｋ）はｅビットの整数である。

ベクトルｍ＝（m_1，m_2，・・・，m_k）　…（８）

【００３８】

〈伸長変換〉

メッセージベクトルｍを、各成分がｅビットの整数であるｋ次元ベクトルとし、乱数ベクトルｒを、各成分がｅ′ビットの整数であるｎ次元ベクトルとする。但し、ｅ＜ｅ′とする。また、ベクトルｓを、重みｋの（ｋ＋ｎ）次元の２値ベクトルとする。このベクトルｓを「位置特定子」と称する。

【００３９】

ｈを下記（９）のように設定し、ベクトルｓ′を（ｈｅ－（ｋ＋ｎ））ビットの任意の２値詰め物ベクトルとする。ｈｅ次元の２値連接ベクトル［ベクトルｓ｜ベクトルｓ′］は、各成分がｅビットの整数である下記（10）のようなｈ次元のベクトルｔに分割できる。

【００４０】

【数７】

$$h = \lceil (k+n) / e \rceil \quad \cdots (9)$$

$$\vec{t} = (t_1, t_2, \cdots, t_h) \quad \cdots (10)$$

【００４１】

Ｋ＝ｋ＋ｎ＋ｈとし、各添数集合I_N，I_R及びI_Lを夫々下記（11），（12）及び（13）のように定義する。但し、バーベクトルｓはベクトルｓのビット補数を表す。

【００４２】

【数８】

$$I_N = Ind(\vec{s}) \quad \cdots (11)$$

$$I_R = Ind(\overline{\vec{s}}) \quad \cdots (12)$$

$$I_L = \{k+n+1, k+n+2, \cdots, K\} \quad \cdots (13)$$

【００４３】

なお、上記例では添数集合I_Lの成分を最後尾のｈ個としたが、これらの成分の位置は任意であって良い。このような場合、下記（14），（15）の条件を満たし、ベクトルｍ′，ベクトルｓは夫々下記（16），（17）のように表される。

【００４４】

【数９】

$$I_N \cup I_R \cup I_L = \{1, 2, \cdots, K\} \quad \cdots \quad (14)$$

$$I_N \cap I_R = I_R \cap I_L = I_L \cap I_N = \phi \quad \cdots \quad (15)$$

$$\vec{m'} = \vec{m}\{Vec\ (I_N, K)\} + \vec{r}\{Vec\ (I_R, K)\} + \vec{t}\{Vec\ (I_L, K)\} \quad \cdots \quad (16)$$

$$\vec{s} = Vec\ (I_N, K)\ [\overline{Vec\ (I_L, K)}] \quad \cdots \quad (17)$$

【００４５】

メッセージベクトルｍを、下記（18）のように、伸長メッセージベクトルｍ′＝（m_1'，m_2'，・・・，m_K'）に変換する。この際、このベクトルｍ′の各成分の大きさは下記（19）である。

【００４６】

【数１０】

$$\vec{m'} = [\vec{m}\ \{\vec{s}\} + \vec{r}\ \{\overline{\vec{s}}\}\ |\vec{t}] \quad \cdots \quad (18)$$

$$|m_i'| = \begin{cases} e & (i \in I_N \cup I_L) \\ e' & (i \in I_R) \end{cases} \quad \cdots \quad (19)$$

【００４７】

〈鍵生成〉

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$，$\{v_i^{(P)}\}$，$\{v_i^{(Q)}\}$，
P，Q，N，w（但し、i＝1，2，・・・，K）

・公開鍵：ベクトルｃ＝（c_1，c_2，・・・，c_K），I_L，e，e′

なお、上記Ｎは公開であっても良い。

【００４８】

まず、任意のｉ，ｊ（但し、ｉ≠ｊ）について、下記（20）～（23）の条件を満たすような２組の基数｛$d_i^{(P)}$｝，｛$d_i^{(Q)}$｝を生成する。

【００４９】

【数１１】

$$gcd(d_i^{(P)}, d_j^{(P)}) = 1 \quad \cdots \quad (20)$$

$$gcd(d_i^{(Q)}, d_j^{(Q)}) = 1 \quad \cdots \quad (21)$$

$$gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \quad \cdots \quad (22)$$

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \cdots \quad (23)$$

【００５０】

$v_i^{(P)}$，$v_i^{(Q)}$をランダムな整数として、下記（24），（25）のように、$V_i^{(P)}$，$V_i^{(Q)}$を導く。但し、$v_i^{(P)}$及び$v_i^{(Q)}$は、下記（26）及び（27）の条件を満たす。

【００５１】

【数１２】

$$V_i^{(P)} = \frac{d_1^{(P)} d_2^{(P)} \cdots d_k^{(P)}}{d_i^{(P)}} v_i^{(P)} \quad \cdots \quad (24)$$

$$V_i^{(Q)} = \frac{d_1^{(Q)} d_2^{(Q)} \cdots d_k^{(Q)}}{d_i^{(Q)}} v_i^{(Q)} \quad \cdots \quad (25)$$

$$gcd(d_i^{(P)}, v_i^{(P)}) = 1 \quad \cdots \quad (26)$$

$$gcd(d_i^{(Q)}, v_i^{(Q)}) = 1 \quad \cdots \quad (27)$$

【００５２】

次に、任意の伸長メッセージベクトルｍ′について条件$M_P < P$，$M_Q < Q$を満たすような大きな素数Ｐ，Ｑを設定する。なお、M_P，M_Qは夫々下記（28），（29）で定義される。

【００５３】

【数１３】

$$M_P = m'_1 V_1^{(P)} + m'_2 V_2^{(P)} + \cdots + m'_K V_K^{(P)} \quad \cdots \quad (28)$$

$$M_Q = m'_1 V_1^{(Q)} + m'_2 V_2^{(Q)} + \cdots + m'_K V_K^{(Q)} \quad \cdots \quad (29)$$

【００５４】

そして、Ｎ＝ＰＱを設定し、中国人の剰余定理によりV_i（$0 \leqq V_i < N$）を下記（30）により計算する。

【００５５】

【数１４】

$$V_i \equiv \begin{cases} V_i^{(P)} & (\mathrm{mod}\ P) \\ V_i^{(Q)} & (\mathrm{mod}\ Q) \end{cases} \quad \cdots \quad (30)$$

【００５６】

公開鍵ベクトルｃの各成分を、下記（31）により求める。ここでｗは、Z_N^*から任意に選ばれた乱数である。

$$c_i \equiv w V_i \quad (\mathrm{mod}\ N) \quad \cdots (31)$$

【００５７】

〈暗号化〉

エンティティａ側（送信側）で、前述した位置特定子であるベクトルｓを任意に生成する。即ち、メッセージベクトルｍに関する位置を示す添数集合I_Nを、送信者であるエンティティａは任意に選択する。次に、エンティティａ側（送信側）で、各成分が任意に選択されたｅ′ビットの整数からなるｎ次元のベクトルｒを生成する。この乱数ベクトルｒにより、高密度が実現される。つまり、冗長部分（退化部分）である乱数ベクトルｒの付加によって、後述するように密度が高くなる。

【００５８】

エンティティａ側（送信側）で、メッセージベクトルｍを、ベクトルｓ及びベクトルｒによって、伸長メッセージベクトルｍ′に変換する。そして、この伸長メッセージベクトルｍ′と公開鍵ベクトルｃとの内積を下記（32）のように求めて、暗号文Ｃを得る。作成された暗号文Ｃは通信路３を介してエンティティａからエンティティｂへ送信される。

【００５９】

【数１５】

$$C = \vec{m'} \cdot \vec{c} = m'_1 c_1 + m'_2 c_2 + \cdots + m'_K c_K \quad \cdots \quad (32)$$

【００６０】

この暗号化にあっては、暗号化すべき平文を分割したメッセージベクトルｍは、添数集合I_Nにて示される位置で伝送され、添数集合I_Nの情報は、添数集合I_Lにて示される位置でベクトルｓによって伝送される。

【００６１】

〈復号〉

エンティティｂ側（受信側）で、以下のようにして復号処理が行われる。

中間メッセージＭは、下記（33）を満たす。従って、法Ｐ，法Ｑにおける中間メッセージM_P，M_Qは、下記（34），（35）のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{N} \quad \cdots (33)$$

$$M_P \equiv M \pmod{P} \quad \cdots (34)$$

$$M_Q \equiv M \pmod{Q} \quad \cdots (35)$$

【００６２】

そして、下記（36），（37）によって（$m_i^{(P)}$，$m_i^{(Q)}$）を求め、中国人の剰余定理を適用することにより、下記（38）が成立して、メッセージベクトル$m'' = (m_1'', m_2'', \cdots, m_K'')$を復号することができる。

【００６３】

【数１６】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \quad \cdots \quad (36)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \quad \cdots \quad (37)$$

$$m_i'' \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \quad \cdots \quad (38)$$

【００６４】

e′＞eであるので，復号されたメッセージベクトルm″の各成分は、上記（19）から、下記（39）の条件を満たす。

【００６５】

【数１７】

$$\begin{cases} m_i'' = m_i' & (i \in I_N \cup I_L) \\ m_i'' \neq m_i' & (i \in I_R) \end{cases} \quad \cdots \quad (39)$$

【００６６】

添数集合I_Lに従って、下記（40）のように、復号ベクトルm″からベクトルtを取り出す。

【００６７】

【数１８】

$$\vec{t} = \vec{m''}\,[\mathrm{Vec}\,(I_L, K)] \quad \cdots \quad (40)$$

【００６８】

ベクトルtをｈｅ次元の２値ベクトル［ベクトルｓ｜ベクトルｓ′］と見なすことにより、（ｋ＋ｎ）次元で重みｋの２値ベクトルｓをエンティティｂ側（受信側）で再構築できる。よって、最終的に、下記（41）のように、メッセージベクトルｍを得ることができる。

【００６９】

【数１９】

$$\vec{m} = \vec{m''}\ [\vec{s}] \quad \cdots \quad (41)$$

【００７０】

なお、添数集合I_Lの成分を任意とする一般的な場合には、上記（41）において、ベクトルm″を下記（42）に示すものに代えることにより、メッセージベクトルmが得られる。

【００７１】

【数２０】

$$\vec{m''}\ \overline{[Vec\ (I_L, K)]} \quad \cdots \quad (42)$$

【００７２】

次に、上述したような本発明の暗号化方式における安全性について述べる。密度が0.9408より小さい場合には、本発明のような積和型公開鍵暗号はＬＬＬアルゴリズムに基づく低密度攻撃によって破られることが知られている。上述した本発明の暗号化方式では、１を超える高い密度を実現できており、このことはこの方式が低密度攻撃に対して安全であることを示している。

【００７３】

乱数$v_i^{(P)}$，$v_i^{(Q)}$を何れもｆビットとした場合、上述した本発明の暗号化方式における密度ρは、下記（43）の条件を満たす。但し、Ｋ＝ｋ＋ｎ＋ｈ，ｅ′＞ｅである。

【００７４】

【数２１】

$$\rho > \frac{(k+h)\ e+n e'}{e'+\log_2 N+\log_2 n}$$

$$> \frac{Ke+n\ (e'-e)}{Ke+\ (3e'-e)\ +f+1+3\log_2 n} \quad \cdots \quad (43)$$

【００７５】

例えば、ここで簡単のために、ｆ＝ｅ，ｅ′＝２ｅと設定した場合、ｎは下記（44）の条件を満たすので、ρ＞１を実現できている。現実的な例として、ｅ＝32とした場合、何れのｋについてもｎ＝７とすることにより、ρ＞１を達成できることが分かる。

【００７６】

【数２２】

$$(n-6)\,e>3\log_2 n+1 \quad \cdots \quad (44)$$

【００７７】

また、本発明の暗号化方式では、高いレートも実現できている。上述した本発明の暗号化方式におけるレートηは、下記（45）の条件を満たす。

【００７８】

【数２３】

$$\eta = \frac{ke}{\lceil e'+\log_2 N+\log_2 n\rceil} > \frac{ke}{Ke+(3e'-e)+f+1+3\log_2 n} \quad \cdots \quad (45)$$

【００７９】

ここで簡単のために、ｆ＝ｅ，ｅ′＝２ｅと設定した場合、ｎ及びｋは下記（46）の条件を満たすので、η＞0.5 を実現できている。現実的な例として、ｅ＝32とした場合、ｎ＝７でｋ＞14とすることにより、η＞0.5 を達成できることが分かる。例えば、ｋ＝57とした場合に、η≒0.7884となる。このように、レートの観点から見ても、本発明の方式は効率的である。

【００８０】

【数２４】

$$\left(k-n-\left\lceil\frac{k+n}{e}\right\rceil-6\right)e>3\log_2 n+1 \quad \cdots \quad (46)$$

【００８１】

本発明の暗号化方式では、高い密度を実現できるため、低密度攻撃に対し、十分に安全である。また、送信側のエンティティにおいて、退化基数の位置を自由に決定できる。よって、位置が分かっている退化基数に基づき、攻撃者が本発明の暗号化方式に対して有効な攻撃を行おうとした場合でも、その攻撃者にとって退化基数の位置を同定することが困難である。従って、退化基数の位置が固定ではなく送信側で任意に決定できるという本発明の特徴は、退化基数の位置が既知である場合に有効である攻撃に対しても安全であることを示している。

【００８２】

以下、本発明の他の実施の形態について説明する。上述した例では全てのブロックにおいて、I_L の位置を固定（最後尾）としているが、この I_L の位置は各ブロックにおいて異なっていても良い。このような例として、以下のようなものが可能である。

【００８３】

（第１例）

最初のブロックについては I_L の位置を固定（例えば上述した例と同様に最後尾）し、この I_L は公開しておく。そして、２番目以降のブロックについては、１つ前のブロックのメッセージベクトルよりそのブロックの I_L の位置を決定するようにする。よって、２番目以降のブロックからは、I_L の位置が変動する。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックの I_L は公開されており、しかも、２番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックの I_L の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。この第１例では、各ブロックにおいて I_L の位置を変動させるため、安全性

の向上を図れる。

【００８４】

（第２例）

最初のブロックについてはI_Lの位置を固定（例えば上述した例と同様に最後尾）し、このI_Lは公開しておく。そして、２番目以降のブロックについては、I_Lの項を設けないようにし、I_Lの項に割り当てられるｈ次元のベクトルを平文を分割したメッセージに割り当てる。そして、この２番目以降のブロックについては、１つ前のブロックのメッセージよりそのブロックにおける退化基数の位置を示す位置情報を決定する。よって、２番目以降のブロックには、I_Lが存在しない。このようにして、送信側のエンティティが退化基数の位置を任意に決定しても最初のブロックのI_Lは公開されており、しかも、２番目以降のブロックでは前のブロックのメッセージベクトルからそのブロックでの退化基数の位置が分かるので、受信側のエンティティにおいて、上述した例と同様に、暗号文から平文を復号できる。また、２番目以降のブロックではメッセージに割り当てる部分がｋ項から（ｋ＋ｈ）項に増えるので、１ブロック内に盛り込めるメッセージ量が増加して、レートをより高くすることができる。

【００８５】

なお、上記例では、暗号化すべき平文を分割したメッセージベクトルｍの各成分の位置（添数集合I_N）を示す情報（添数集合I_L）を伝送するようにしたが、付加する乱数ベクトルｒの各成分の位置（添数集合I_R）を示す情報を伝送するようにしても良いことは勿論である。

【００８６】

また、上記例では、２組の基数$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$に乱数$\{v_i^{(P)}\}$，$\{v_i^{(Q)}\}$を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【００８７】

また、上記例では、Ｋ個の要素からなる基数の集合$\{d_i\}$を２組（$\{d_i^{(P)}\}$，$\{d_i^{(Q)}\}$）生成する多重化した方式の場合について説明したが、１組の基数の集合$\{d_i\}$を用いる方式についても、本発明を同様に適用できること

は勿論である。

【００８８】

図２は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、上述した暗号化方式の手順に従って伸長平文ベクトルｍ′を得る処理と、得た伸長平文ベクトルｍ′と公開鍵ベクトルｃとの内積計算により暗号文Ｃを作成する処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、送信側のエンティティに設けられている。

【００８９】

図２において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばＷＷＷ(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11a が記録されている。記録媒体11から通信線等の伝送媒体14を介して読み出されたプログラム11a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００９０】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体12には前述の如きプログラム12a が記録されている。記録媒体12から読み出されたプログラム12a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００９１】

コンピュータ10に設けられたディスクドライブ10a に装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体13には前述の如きプログラム13a が記録されている。記録媒体13から読み出されたプログラム13a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００９２】

【発明の効果】

以上のように、本発明では、暗号化すべき平文を分割してなる第１ベクトル（

平文ベクトル）、特に暗号化を必要としない乱数成分からなる第２ベクトル（疑似平文ベクトル）、及び、第１ベクトルまたは第２ベクトルの各成分の位置を示す第３ベクトル（位置特定ベクトル）を合わせた第４ベクトル（伸長平文ベクトル）と、公開されている第５ベクトル（公開鍵ベクトル）とを用いて暗号文を作成する。具体的には、第４ベクトル（伸長平文ベクトル）の各成分と、１または複数の第６ベクトル（基数ベクトル）を基にモジュラ変換した第５ベクトル（公開鍵ベクトル）の各成分との積和演算によって暗号文を構成し、第１ベクトルまたは第２ベクトルの各成分の位置を、暗号文を作成する送信側のエンティティで決定するようにしたので、暗号化が必要でない冗長部分（退化部分）を付加しているため、暗号文の密度を大きくでき、ＬＬＬアルゴリズムに基づく低密度攻撃に対して強くなって安全性を向上でき、また、暗号化すべき平文部分の位置または冗長部分（退化部分）の付加位置は、固定でなく、送信側のエンティティが任意に決定できるため、攻撃者にとってその位置を見つけることすら困難であり、安全性の更なる向上を図れる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図２】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

１　暗号化器

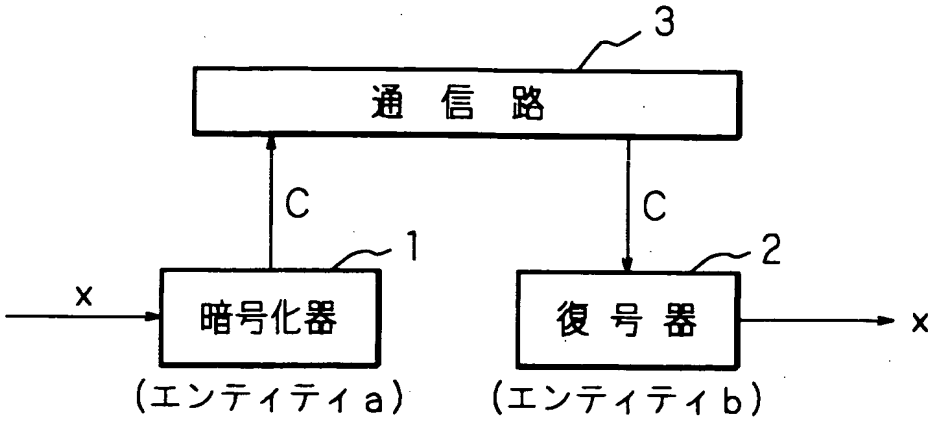
２　復号器

３　通信路

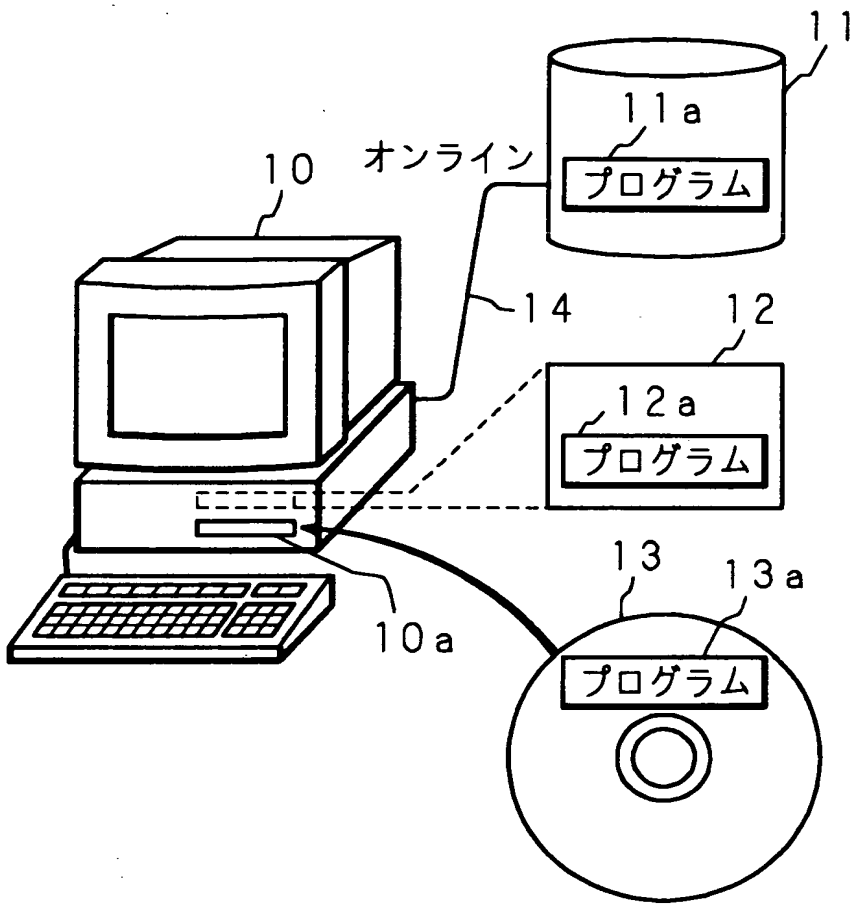
ａ，ｂ　エンティティ

【書類名】　　図面

【図１】



【図２】



【書類名】　　要約書

【要約】

【課題】　ＬＬＬアルゴリズムに基づく低密度攻撃に強く、安全性を向上できる暗号化方式を提供する。

【解決手段】　暗号化すべき平文を分割した平文ベクトル、任意の乱数成分からなる疑似平文ベクトル、及び、平文ベクトルまたは疑似平文ベクトルの成分の位置を特定する情報を有する位置情報ベクトルを加えた伸長平文ベクトルの各成分と、１または複数組の整数d_i（$1 \leqq i \leqq K$）及び乱数v_iを用いて$V_i = (d / d_i) \cdot v_i$（但し、$d = d_1 d_2 \cdots d_K$（任意の２つの整数$d_i$，$d_j$は互いに素））に設定された１または複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得る。平文ベクトルまたは疑似平文ベクトルの成分の位置は、送信側（エンティティａ）が決定する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄